GIOIELLERIA GATTOPARDO

DI LENNY ARTALE

Misure minime di sicurezza per la protezione dei dati personali, sensibili e/o giudiziari

(art.33-34-35-36 del Codice Privacy)

Sommario

Premessa

Le presenti istruzioni costituiscono una serie organica di indirizzi, orientate a garantire la sicurezza dei dati e delle informazioni detenute dagli uffici e dalle strutture della Gioielleria Artale Lenny
Per misure di sicurezza deve intendersi l'insieme delle prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un adeguato livello di sicurezza nel trattamento dei dati e sono volte a ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei dati,
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta,
- modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole.

I dati e le informazioni di carattere sensibile devono essere trattati in aree protette dall'accesso di persone non autorizzate. Quando restano incustodite dal personale autorizzato, le aree di sicurezza devono restare chiuse e con strumenti di controllo atti ad impedire accessi abusivi. Il personale della **"Gioielleria Artale Lenny"** ha accesso ai locali esclusivamente per l'adempimento della prestazione lavorativa. Il personale che espleta servizi strumentali (es.: *pulizia dei locali*) o si occupa della manutenzione e dei servizi accessori, deve essere espressamente autorizzato ad accedere alle aree di sicurezza. Il Titolare e/o i Responsabili del trattamento devono vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o ove vengono trattati dati sensibili o giudiziari.
Devono essere previsti procedure, accorgimenti e strumenti per:

- consentire l'accesso alle aree dove vengono custoditi e trattati i dati al solo personale autorizzato;
- ostacolare l'accesso abusivo ai dati;
- segnalare la presenza di intrusi.

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura dell'Amministratore di Sistema, del Responsabile designato e dell'Incaricato, in caso di trattamento con strumenti elettronici:

a) Sistema di autenticazione informatica per accesso alla rete della Gioelleria di Artale Lenny
Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato **(user-ID)** associato a una parola chiave riservata (**password**) conosciuta solamente dal medesimo ed a uso esclusivo dell'incaricato. Le user-ID e password individuali per l'accesso alle applicazioni non devono essere mai condivise con altri soggetti, anche se incaricati del trattamento. Nel caso in cui occorre permettere l'accesso da parte di altri utenti, è necessario richiedere la generazione di una nuova password.
Ad ogni incaricato è assegnata individualmente univoca credenziale per l'autenticazione.
Con le istruzioni impartite, a cura dei Responsabili del Trattamento o Amministratore di Sistema, agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale ad uso esclusivo dell'incaricato. la password non va annotata su supporti facilmente rintracciabili e, in particolar modo, in prossimità della postazione di lavoro utilizzata.
La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure; essa non deve contenere riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
Le credenziali di autenticazione non utilizzate da almeno sei mesi vanno disattivate da parte

dell'Amministratore di Sistema, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
Sono impartite istruzioni, da parte dei Responsabili del Trattamento, agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, prevedendo il blocco utente automatico attivabile dopo periodo di inattività.
Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il Responsabile può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

b) Sistema di autorizzazione per l'accesso alla rete della Gioielleria di Artale Lenny

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati dal Responsabile del Trattamento e configurati anteriormente al primo accesso ai sistemi in rete aziendale da parte dell'Amministratore di sistema, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

La lista degli incaricati è aggiornata periodicamente e redatta per classi omogenee di incarico e dei relativi profili di autorizzazione.
I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale a cura dell'Amministratore di Sistema.
Le modalità operative adottate e gli strumenti di protezione posti in essere sono comunicati periodicamente dall'Amm.re di Sistema al Titolare del Trattamento dati.
Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati semestralmente a cura dell'Amministratore di Sistema.
Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale a cura dell'Amministratore di Sistema.

a) Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici posti in essere a cura dell'Amministratore di Sistema.
Sono impartite, a cura dei Responsabili del Trattamento, istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
Sono adottate idonee misure a cura dell'Amministratore di Sistema atte a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.

b) Trattamenti senza l'ausilio di strumenti elettronici

Il trattamento di dati senza strumenti elettronici, coinvolge i dati contenuti nei supporti cartacei o simili che, comunque non richiedano l'uso di elaboratori elettronici. Ove esistano copie o riproduzioni di documenti che contengono dati personali, le medesime devono essere protette con le stesse misure di sicurezza applicate agli originali.
Il Responsabile del trattamento dei dati è tenuto ad effettuare controlli sulle attività degli incaricati del trattamento, al fine di garantire la puntuale applicazione delle disposizioni contenute nel Codice. Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici.
Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.
Per quanto non previsto dal presente documento si rinvia alla normativa vigente in materia.